CTF Final Document:

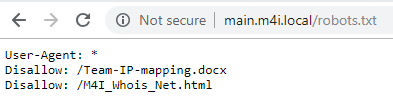
Cover Page

Network Map

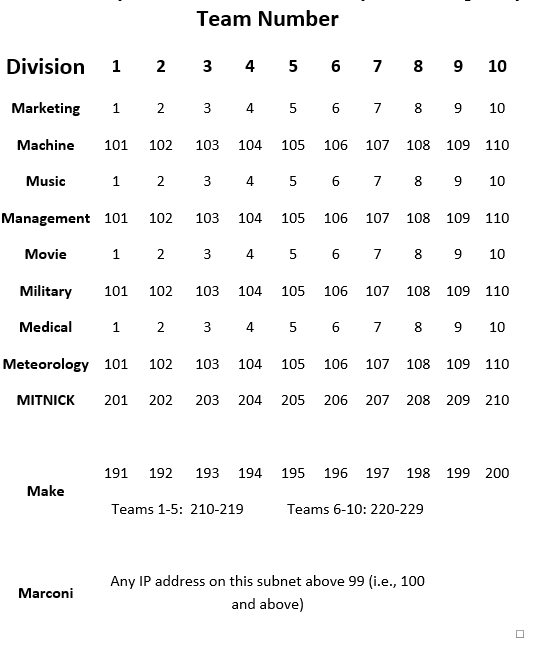
**Marketing Division – 10.1.8.1**

How did you find the target?

* After connecting to main.m4i.local, we learned its IP address was 10.1.8.95. We investigated its Robots.txt page and found the following information:

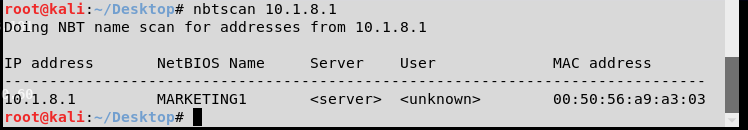


* The Team-IP-mapping.docx contained the final octet of our target’s IP addresses:



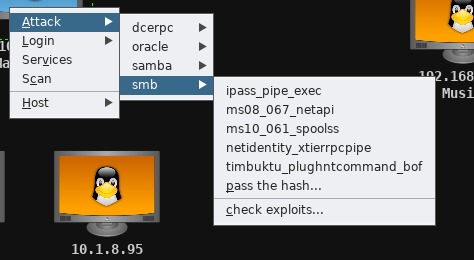
* We then performed an nmap scan of the following IP addresses, using the below nmap command: 10.1.8.1, 10.1.8.101, 10.1.8.201, & 10.1.8.191





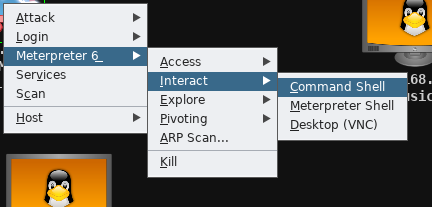
How did you gain access to the target?

* Added the Marketing1 machine to Armitage using an nmap scan – Intense Scan no Ping
* Exploited the machine using the below exploit:

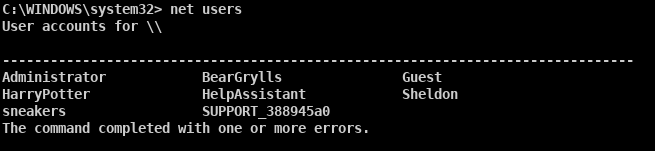


How did you learn usernames?

* On the exploited machine, we opened a command shell using the following options:

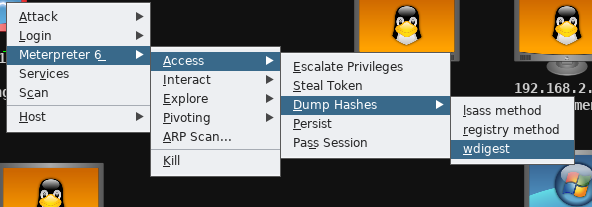


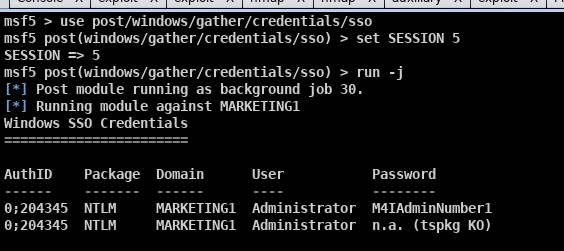
* We ran the net users command to display the list of users:



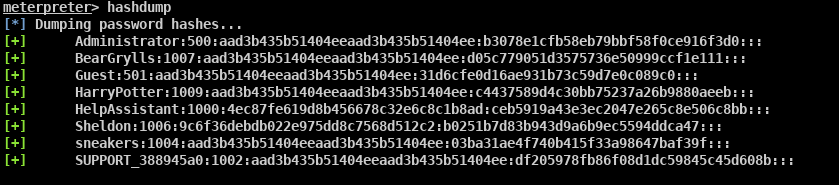
How did you learn passwords?

* To learn the Administrator password, we executed the wdigest command on the exploited machine in Armitage. This gave the below output:

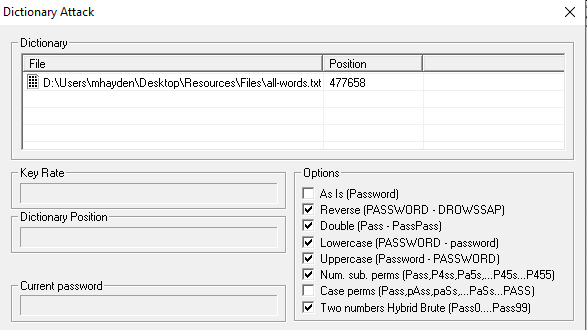




* We then ran a hash dump using the lsass method, with the command shown above highlighted in red. This provided the password hashes shown below:



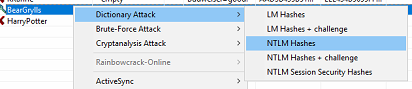
* We input the hash file into Cain, and ran a dictionary attack of all-words.txt, using the following settings:

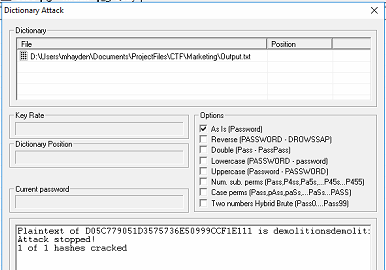


* This found Sheldon’s password of “bigbangtheory”
* We tested the password “Toomanysecrets!” for user sneakers based on the information on the cake in class
* To find BearGryll’s password, we created a wordlist by crawling his biography page using cewl, with the command below:



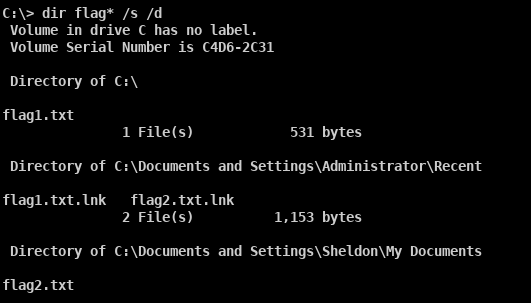
* We ran the Bear\_Wordlist.txt through a python script which duplicated each line, such as changing “Bear” to “BearBearBear”. This python script is included in Appendix B: Source Code.
* We conducted a dictionary attack in Cain of BearGryll’s password, using Output.txt as shown below:



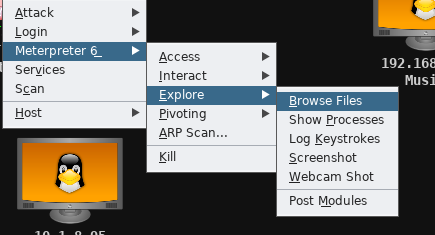


How did you find and download flags?

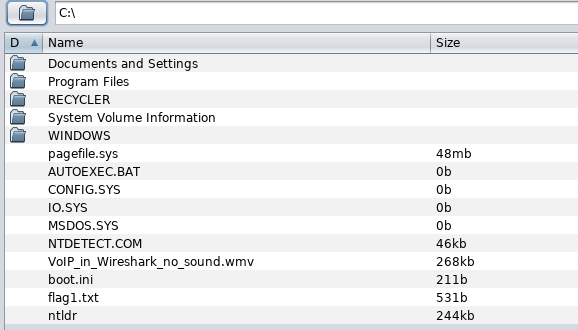
* From the target command prompt in Armitage, we entered the command “dir flag\* /s /d” from the C: directory. This provided the location of flags 1 and 2:



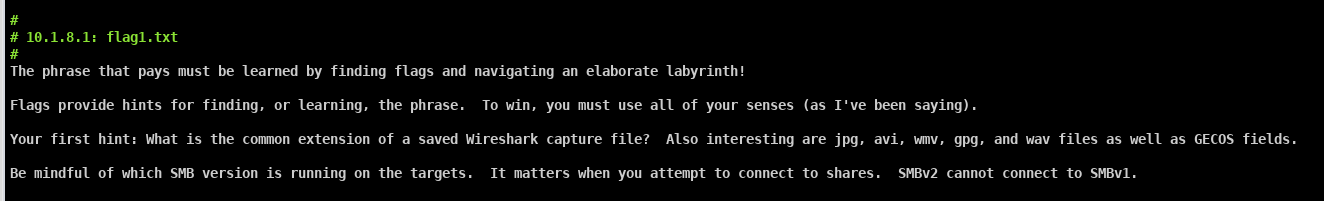
* We downloaded flag1.txt using the Armitage file browser, opened by the following:



* We selected flag1.txt and downloaded it into Armitage:



* Flag1.txt contained the following data:

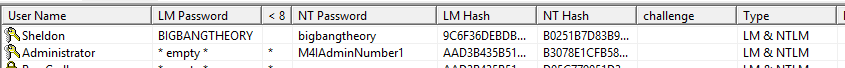


* To download Flag2.txt, we opened a Windows7 VM. We mapped Sheldon’s drive to the local I drive using the net use command outlined in red. From there, we navigated to the locally mapped I drive and opened flag2.txt.



How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
| Administrator | Admin | M4IAdminNumber1 |
| Sheldon |  | bigbangtheory |
| HarryPotter |  |  |
| BearGrylls |  | demolitionsdemolitionsdemolitions |
| sneakers |  | Toomanysecrets! |

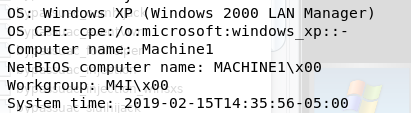


**Machine Division – 10.1.8.101**

How did you find the target?

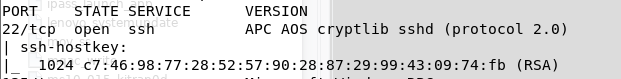
* We ran an nmap scan of IP 10.1.8.101 after using the information regarding the final octet of our target’s IP addresses. The command used is shown below:





How did you gain access to the target?

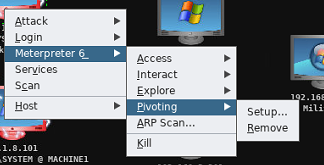
* Port 22 was open which indicated that ssh was a viable attack vector, as shown in our nmap output below.



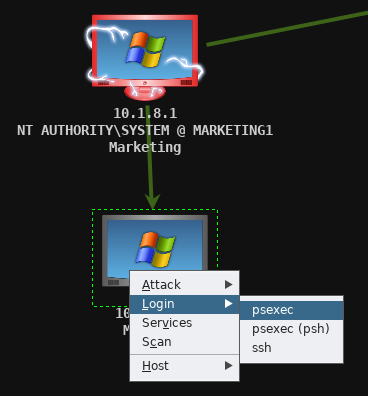
* We used SSH to log in to Machine1 using username “Administrator” and password “M4IAdminNumber2” (discussed in the Password section below).



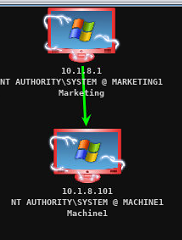
* We selected the previously exploited Marketing1 machine, and setup a pivot.

****

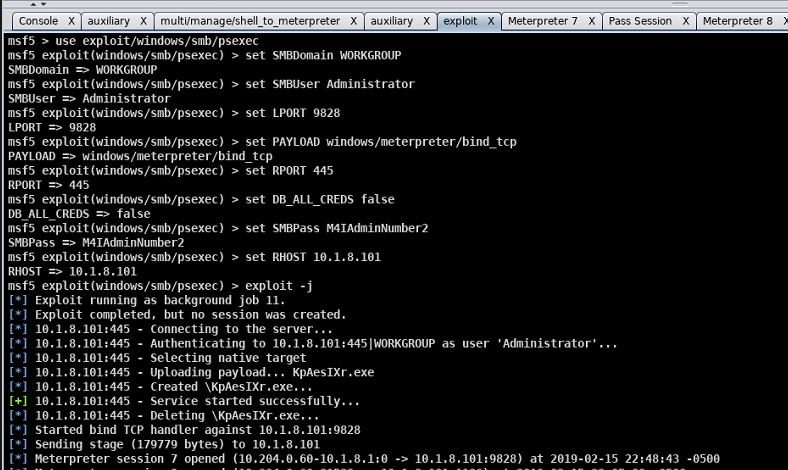
* We then executed the Armitage exploit “windows/smb/psexec**”.** This exploit used the pivot setup above, and then used the Administrator credentials “Administrator:M4IAdminNumber2”.



* The below screenshot shows the bright green arrow, demonstrating that the pivot was in use, and that the machine was exploited.

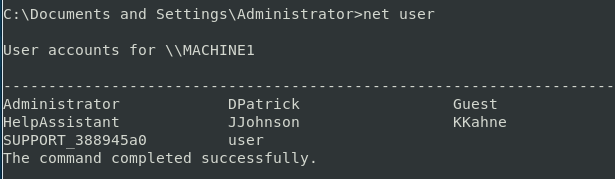
****

* The below screenshot shows the exploit executing in the Armitage window:



How did you learn usernames?

* After using an SSH login with the Administrator account, we ran the “net user” command, showing the below output:

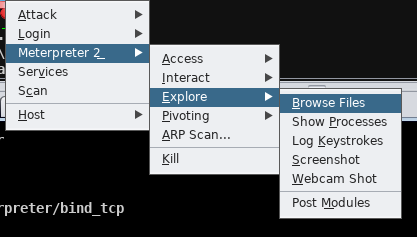


How did you learn passwords?

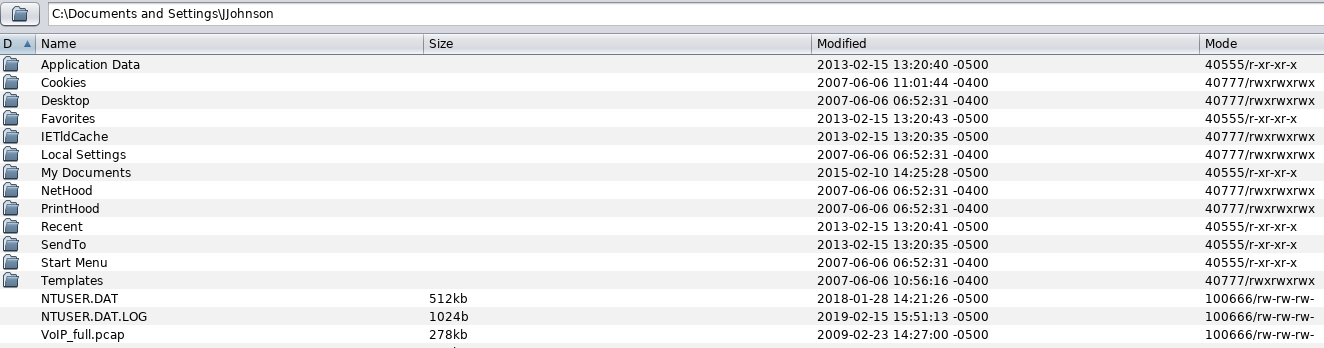
* To learn the Administrator password, we leveraged the cracked password for Marketing1’s Administrator, and used the hint below from the Twitter profile:

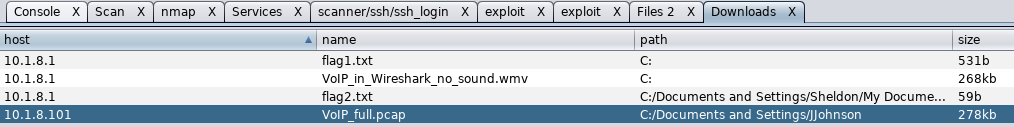


* To find JJohnson’s password, we found a VoIP conversation saved as a .pcap file in the Armitage file browser for Machine1, the extension used by Wireshark.

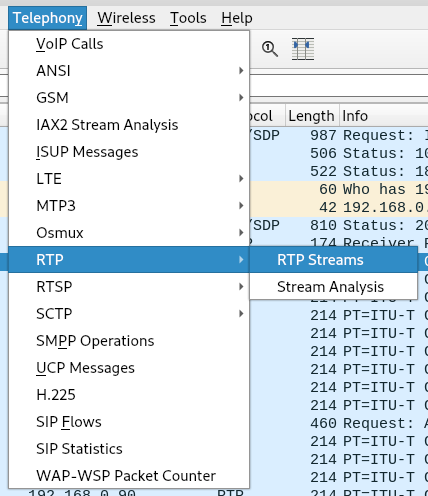


* We opened this file in Wireshark, and listened to the audio stream. He asked the question “What is my password?” To which he received the response “LowesMotorSpeedway” with a capital L, M, and S.

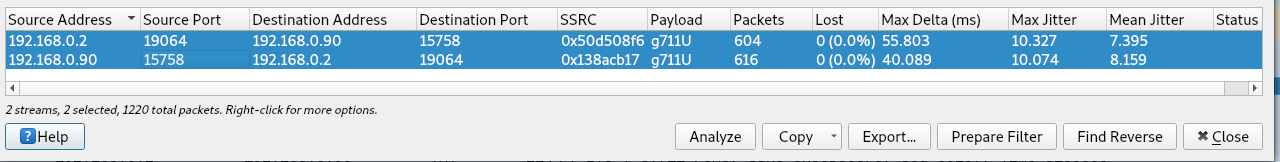




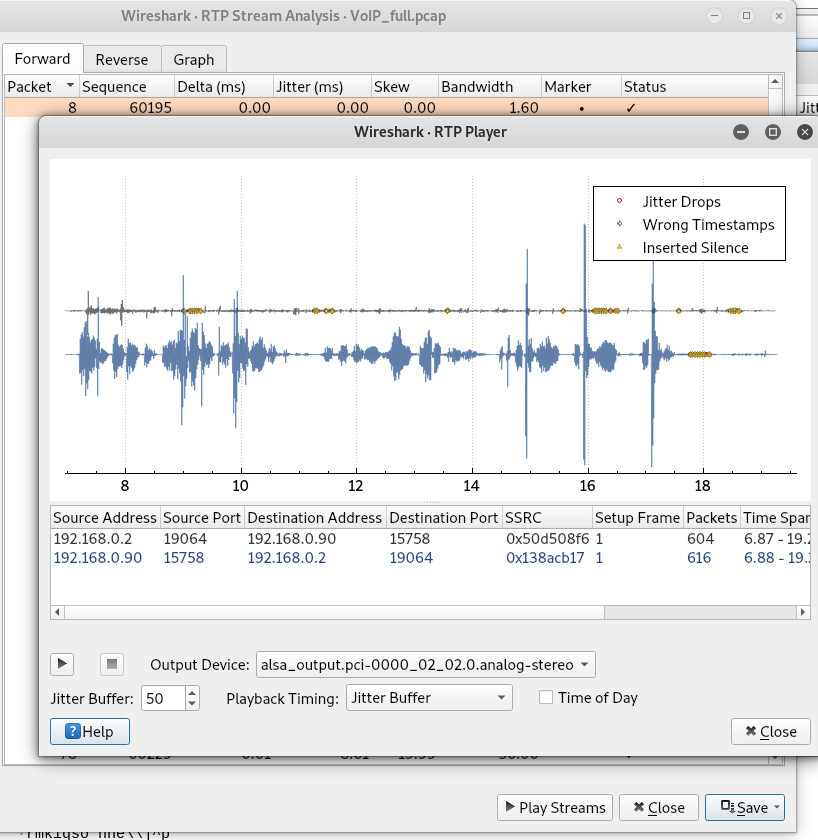
* We opened the PCAP file in a Wireshark window, and selected Telephony 🡪 RTP 🡪 RTP Streams



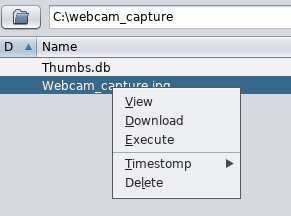
* We highlighted both streams, and selected analyze, outlined below in red.



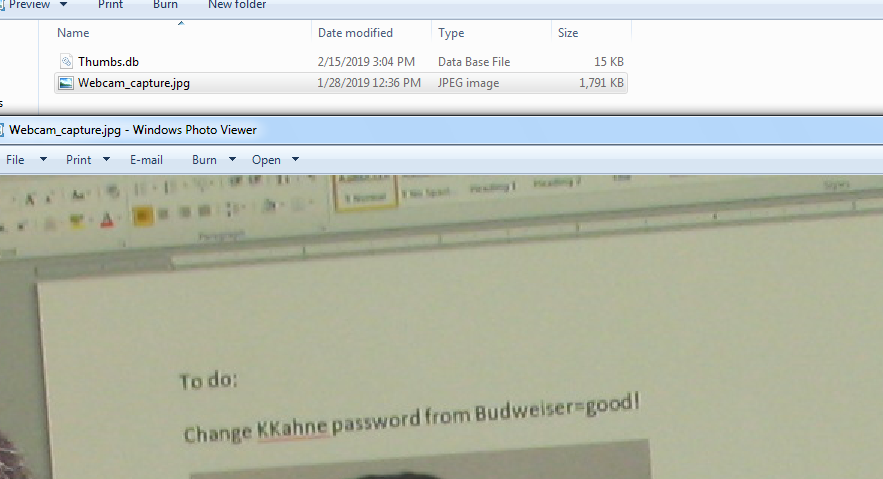
* We then selected play streams, and “play”, and listened to the recording:



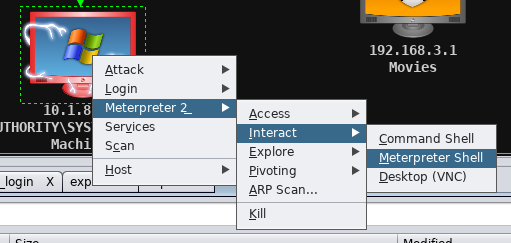
* To find KKahne’s password, we downloaded and opened the webcam\_capture.jpg found at C:\webcam\_capture\Webcam\_capture.jpg, using the Meterpreter file browser.

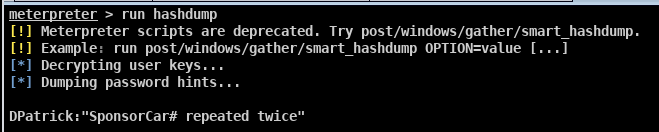


* The webcam capture contained the following note:

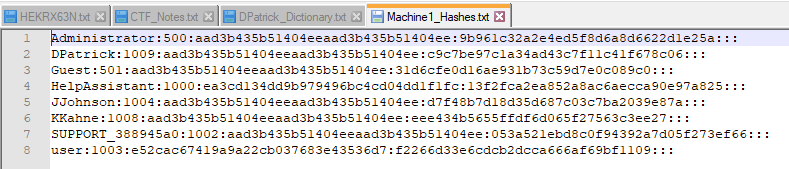


* To find DPatrick’s password, we executed the meterpreter command shown below: “run hashdump”, from a meterpreter shell.

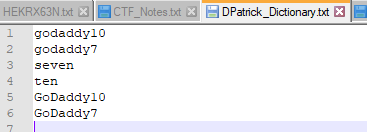




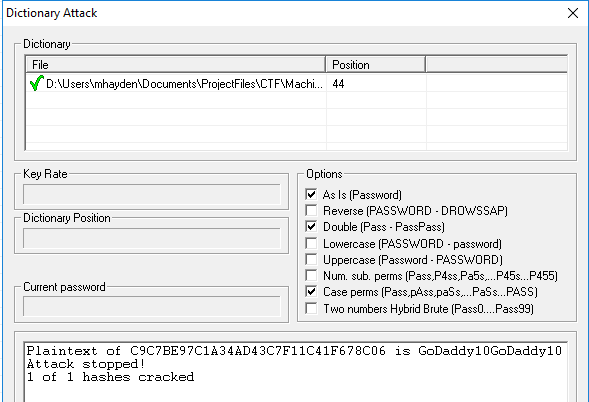
* + We loaded the hashdump file (shown below) into Cain



* + We created a dictionary file of Danika Patrick’s sponsor and number (Go Daddy, and either 10 or 7), shown below:



* + We ran a Cain dictionary search using the above dictionary, with the below settings, to find DPatrick’s password:



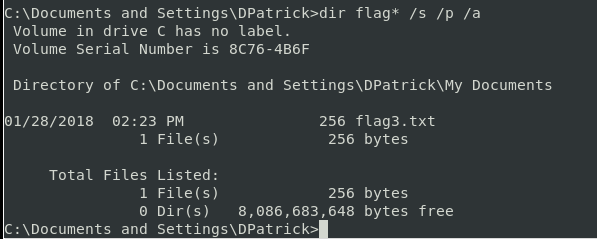
How did you find and download flags?

**Flag3:**

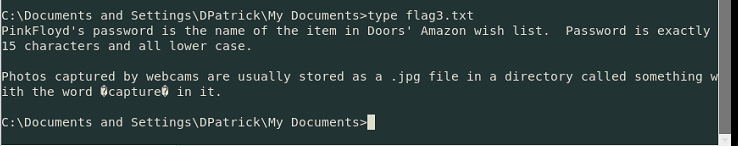
* We opened a ssh connection using the command “ssh DPatrick@10.1.8.101” , and entered the password “GoDaddy10GoDaddy10”.



* We then searched for flag files using the command “dir flag\* /s /p /a”, which gave the flag3.txt location of C:\Documents and Settings\DPatrick\My Documents\flag3.txt

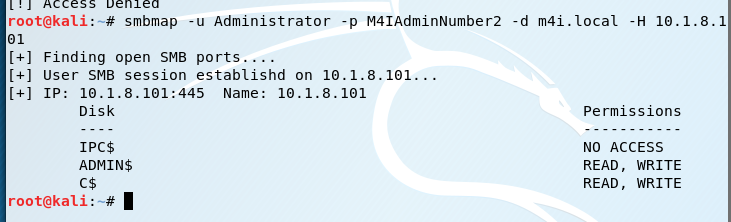


* We navigated to the above directory, and executed the command “type flag3.txt” to display the flag’s contents:

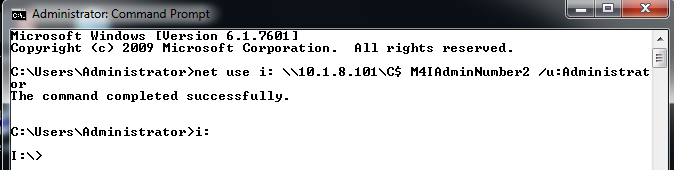


**Flag4:**

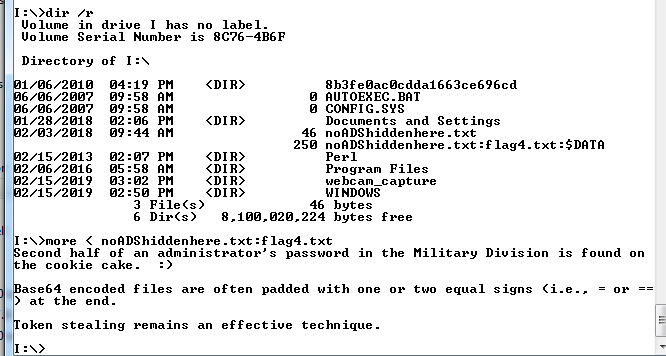
* We viewed the SMB shares onto our computer using the following command:



* We mapped the C$ drive to the local I drive in the Windows 7 VM:



* There was a file “noADShiddenhere.txt”. So we displayed the ADS information using the command “dir /r”, which showed that noADShiddenhere.txt had flag4.txt embedded as ADS information.
* We used the command “more < noADShiddenhere.txt:flag4.txt” to display the flag.



How did you find and download any other files you may have harvested from the target?

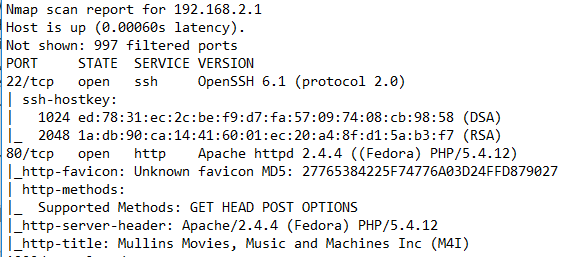
* All other files used from this target were downloaded from the Armitage file browser, shown in the JJohnson password section.

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
| Administrator | Admin | M4IAdminNumber2 |
| DPatrick |  | GoDaddy10GoDaddy10 |
| JJohnson |  | LowesMotorSpeedway |
| KKahne |  | Budweiser=good! |
| user |  | Password!123 |

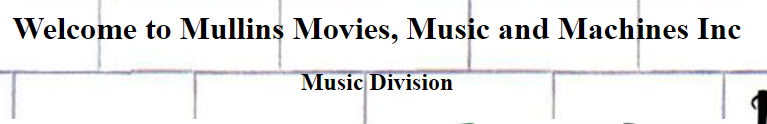
**Music Division – 192.168.2.1**

How did you find the target?

* The nmap output for IP 192.168.2.1 showed that there was an open port 80 – web server.



* We navigated to 192.168.2.1 in a browser, and it was the Music division of M4I.

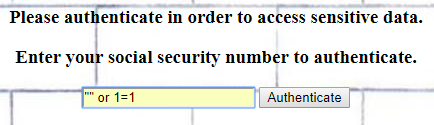


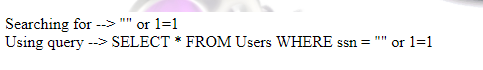
How did you gain access to the target?

* Port 22 was open providing SSH logins
* Port 80 was open providing the web server

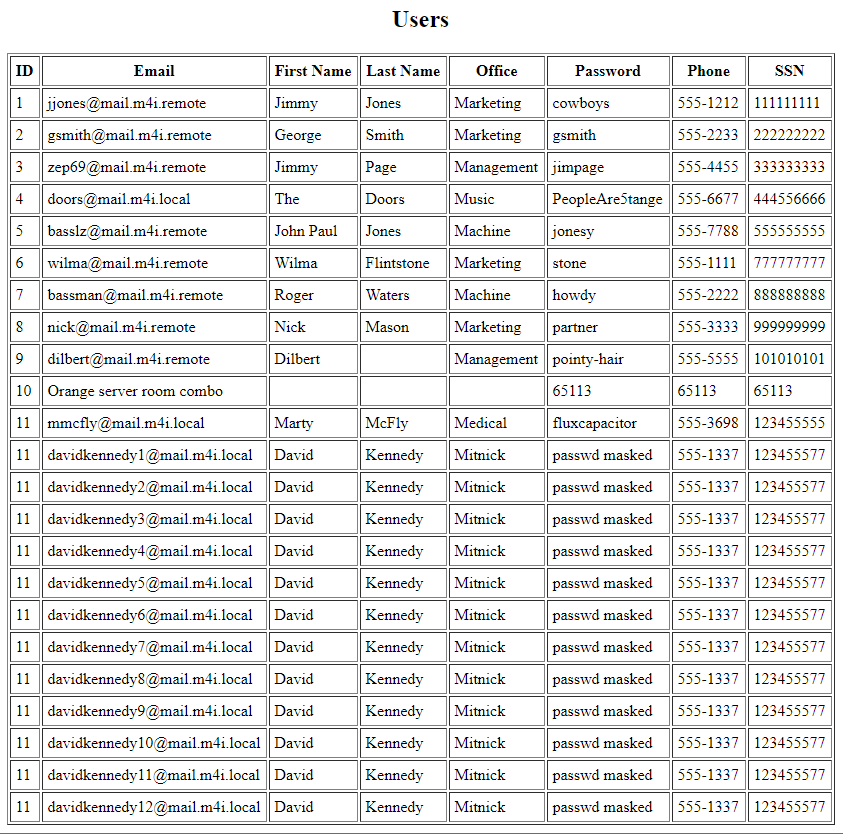
How did you learn usernames?

* We navigated to the Music Division web server. It asked for authentication, so we utilized the below SQL injection:

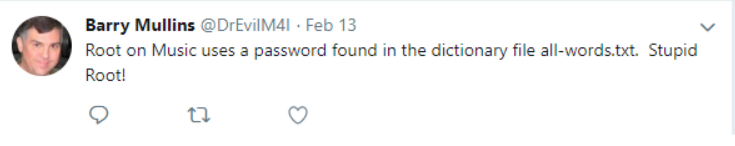




* The table below was given as a result:

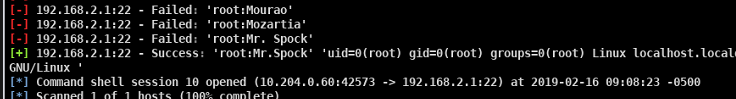


* We used ssh to log into [doors@192.168.2.1](mailto:doors@192.168.2.1):
* The twitter feed for Dr. Evil mentioned the hint below for the root user:

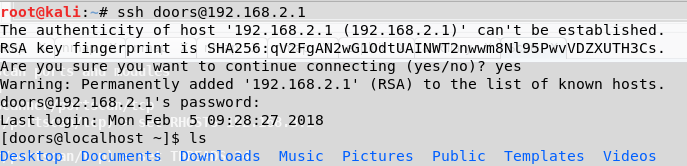


How did you learn passwords?

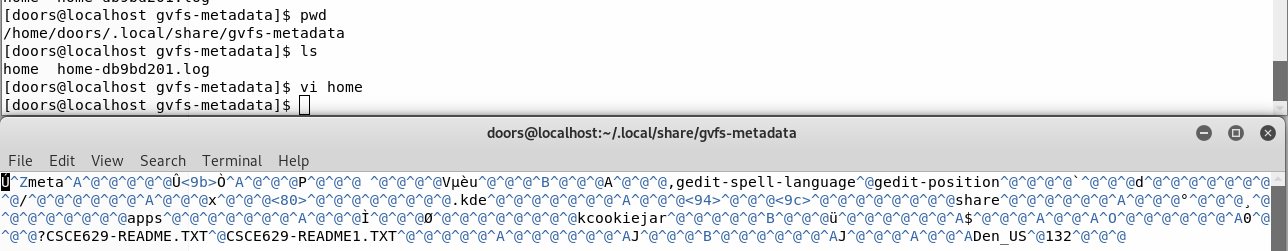
* Doors password was given in the table from the SQL injection
* We found root’s password using a brute force SSH login in Armitage:



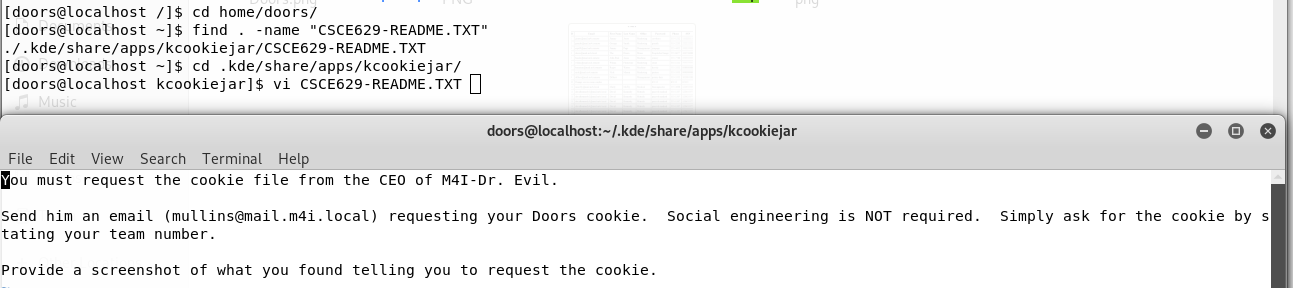
* To find pinkfloyd’s password, flag3 was the starting point: pink floyd’s password is the item in Doors’ Amazon wish list.
  + We used an SSH login to log in as Doors.



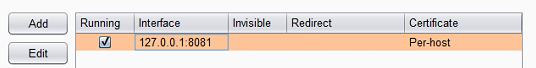
* + We went through various directories on Doors’ machine until the following file was found:



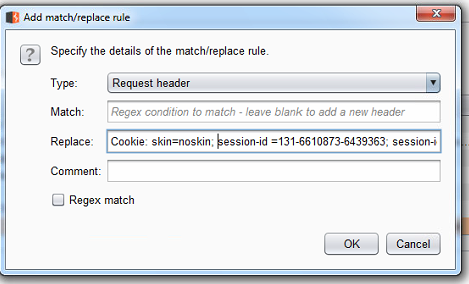
* + We searched for file “CSCE629-README1.TXT”



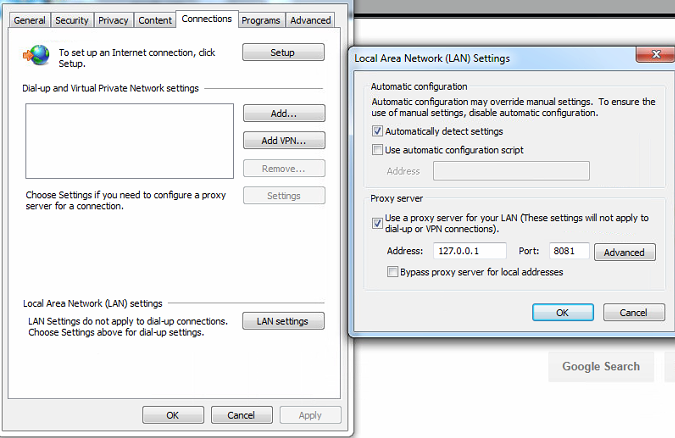
* + We emailed Dr. Evil requesting the cookie file
  + We opened a Burp Proxy to intercept web traffic with the following settings:
    - Listening on loopback interface:



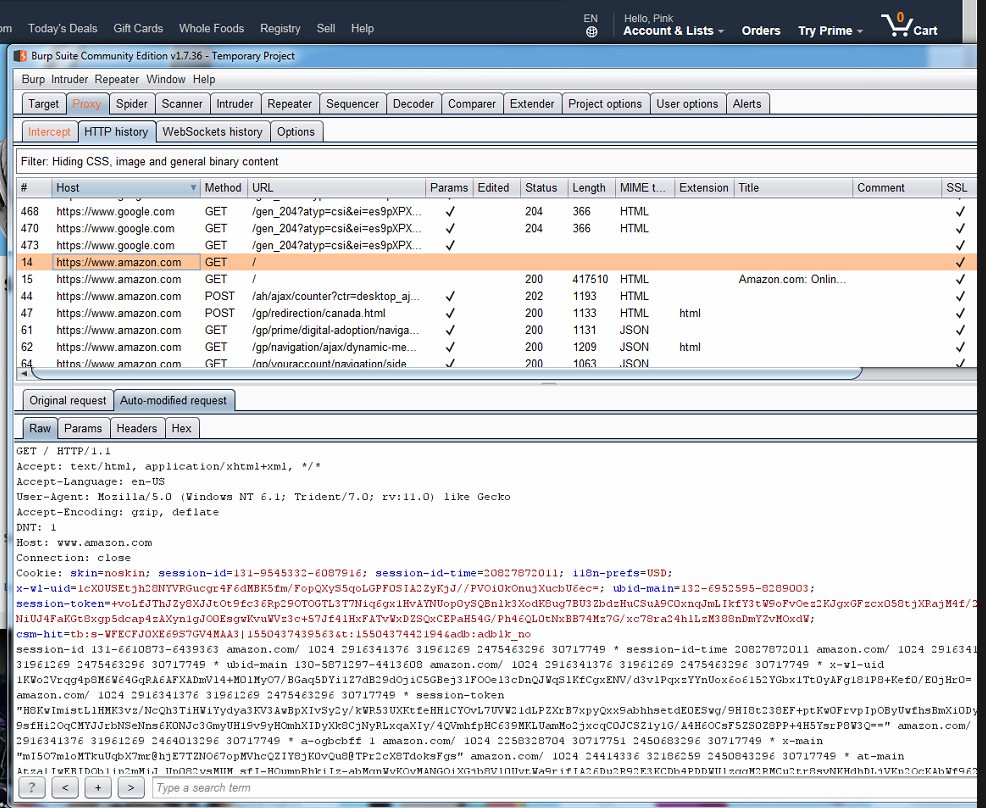
* + - Set up a replacement rule, using all fields from doors’ cookie file:



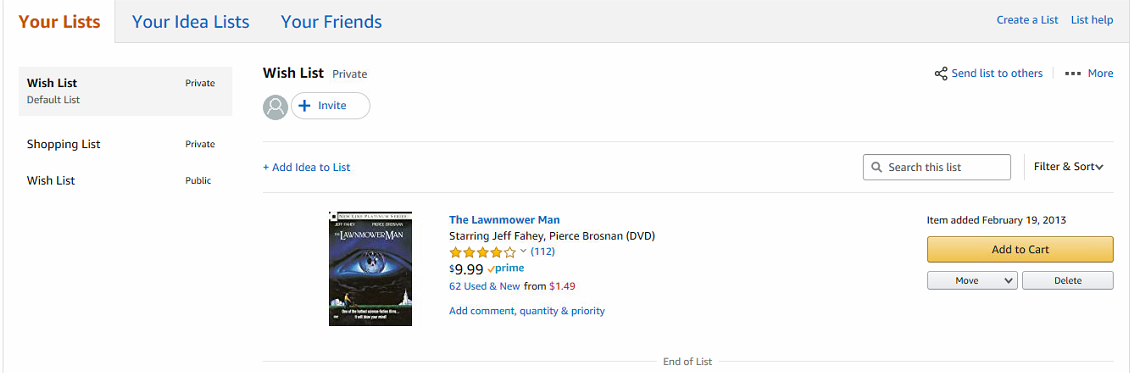
* We configured IE using the below settings to go through the proxy:



* We navigated to Amazon, and intercepted the below HTTP GET, also outlined in red is the Amazon login greeting “Pink”



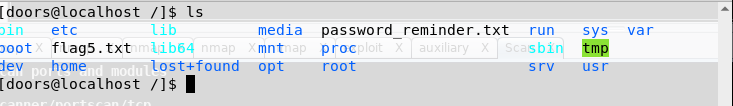
* We navigated to the wish list, and found the following item:



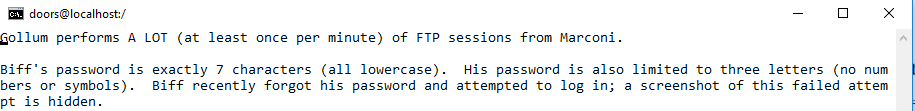
How did you find and download flags?

**Flag5:**

* While SSH’d into the machine as doors, we navigated to the home directory and listed the files, shown below:



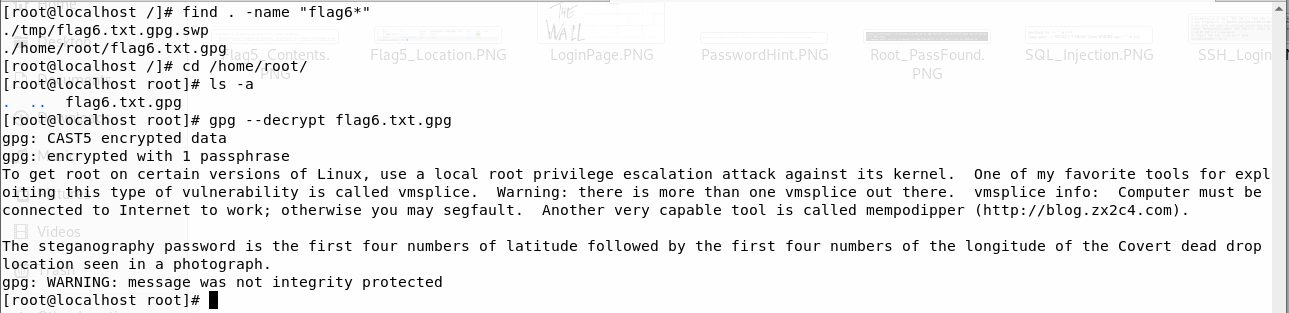
* flag5.txt was in the root directory, shown by the command “vi flag5.txt”



**Flag6:**

* While logged in as root, we searched from the root directory for flag6 using “find . –name “flag6\*”
* This showed a flag6.txt.gpg file.
* We navigated to the flag6.txt.gpg file, and decrypted it using the password “swordfish”, which was shown in the source code of management’s web server (192.168.2.101)





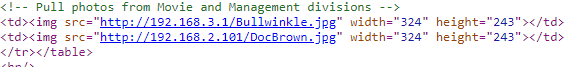
How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
| doors | User | PeopleAre5trange |
| Penny |  |  |
| pinkfloyd |  | thelawnmowerman |
| root |  | Mr.Spock |

**Management Division – 192.168.2.101**

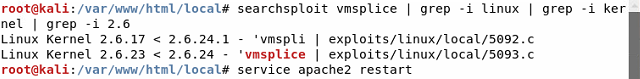
How did you find the target?

* We inspected the page source of main.m4i.local using “ctrl u”. In the page source, two photos were pulled from remote sources, one from the Movie and one from the Management division shown below:

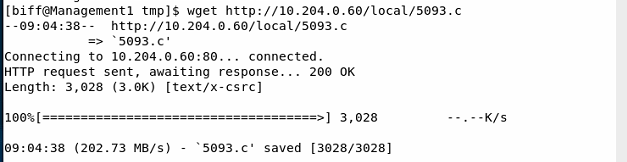


How did you gain access to the target?

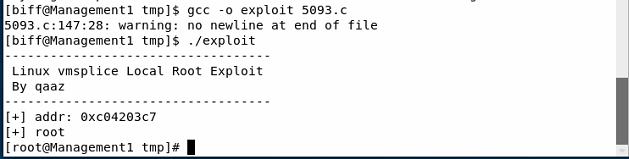
* From the nmap scan, we learned that port 22 – SSH was open. We learned biff’s password as discussed in the password section below and used that to SSH onto the target macine.
* We searched the local exploit database for the vmsplice exploit, shown below, and started an apache webserver on my local machine, also shown highlighted in red.



* We copied the 5093.c file into the /var/www/html/local directory using the command “cp exploits/linux/local/5093.c /var/www/html/local/5093.c”
* From the target machine, we copied the 5093.c exploit into the local /tmp directory, shown below:



* We built the 5093.c exploit into a binary “exploit” using gcc. We executed the exploit using “./exploit”, escalating the connection from biff to root:



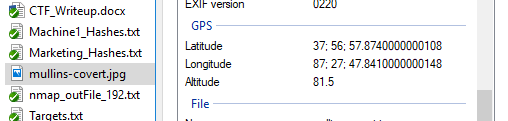
How did you learn usernames?

* Once we gained root access, as displayed above, we executed “cat /etc/passwd” and “cat /etc/shadow”. These output files showed all of the users on the device:

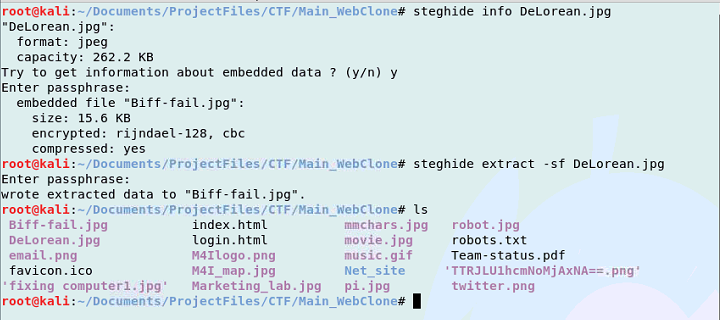


How did you learn passwords?

* We used “steghide info FILENAME” to check each image downloaded from main.m4i.local for embedded information because Flag5 said a failed login was hidden.
  + The password used was “37568727”, the first four digits of the lat/long of mullins-covert.jpg, based on the contents of flag6. The coordinates are shown below:



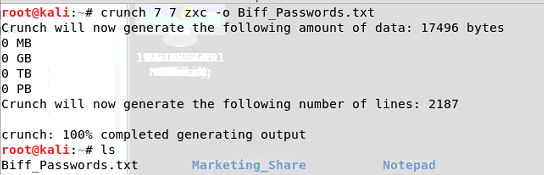
* + Biff-fail.jpg was embedded in DeLorean.jpg, shown below:



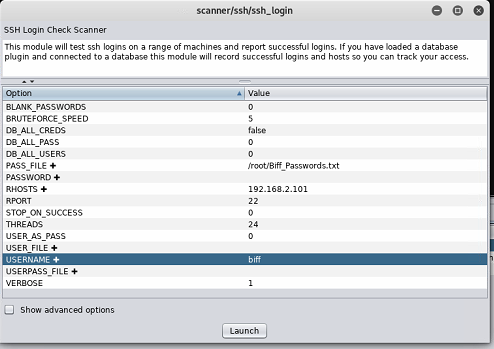
* + Biff-fail.jpg:



* Based on flag5 and Biff-fail.jpg, we used crunch to generate a 7 character password consisting of z, x, and c:



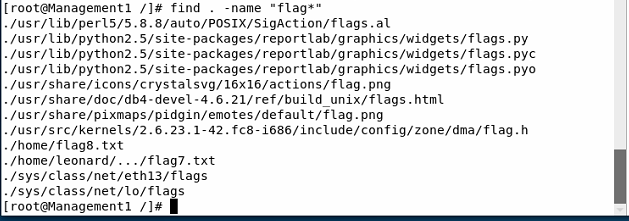
* We then ran a brute force SSH login in Armitage using **auxiliary🡪scanner🡪sshlogin**, using the below settings: producing the correct credential of “zxcczxc”





How did you find and download flags?

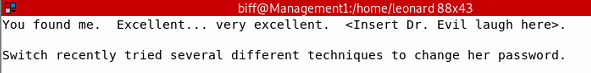
* From the terminal with root access, we executed the command **find . -name “flag\*”**, from the root directory which gave the following locations:



* We viewed both files using vi in the terminal:
  + Flag7 command:



* + Flag7 contents:



* + Flag8 command:



* + Flag8 contents:



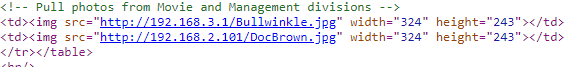
How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
| biff |  | zxcczxc |
| leonard |  | 1cosmos |
| angelabennett |  |  |
| GraceHopper |  |  |
| root |  |  |

**Movie Division – 192.168.3.1**

How did you find the target?

* We inspected the page source of main.m4i.local using “ctrl u”. In the page source, two photos were pulled from remote sources, one from the Movie and one from the Management division shown below:



How did you gain access to the target?

* Once we learned the root password, we used the open port 22 to use an SSH log on.

How did you learn usernames?

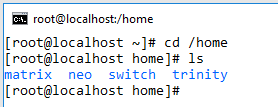
* On the web server for 192.168.3.1, the source showed the following:



* + We entered the shown password into a Hex to ASCII converter, and it produced “Nebuchadnezzar”



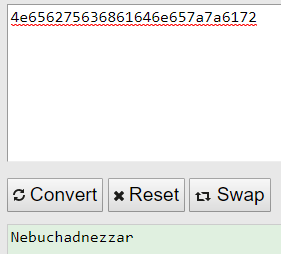
* We logged into the root user using ssh and “Nebuchadnezzar” as the password. We navigated to the /home directory and viewed the users:



How did you learn passwords?

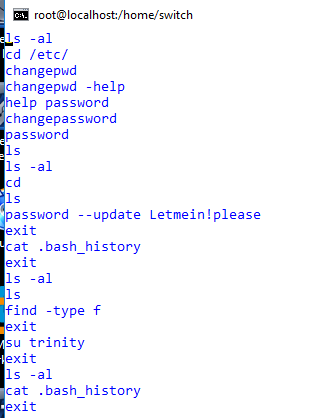
* We learned the root password by converting the hex string into ASCII as shown below:





* From the SSH terminal of the root user, we used the commands “cat /etc/shadow” and “cat /etc/passwd” to view the shadow and password files for use in John.
* We learned switch’s password by checking the .bash\_history file in switch’s directory:

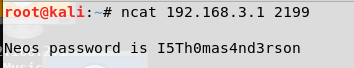




* We found neo’s password by performing an TCP Port scan of the machine. This reported the following information:



* We opened a connection to port 2199, and received the following password:



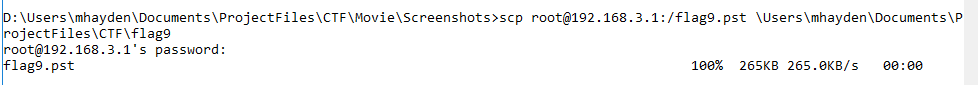
How did you find and download flags?

**Flag9:**

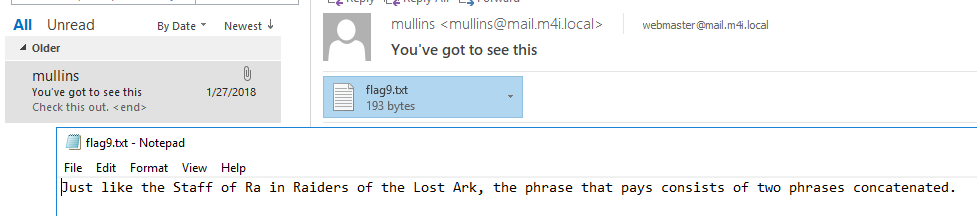
* After using SSH to log into the machine as root, we searched for “flag9” using the below command.



* We transferred the flag9.pst file to a local machine using scp:

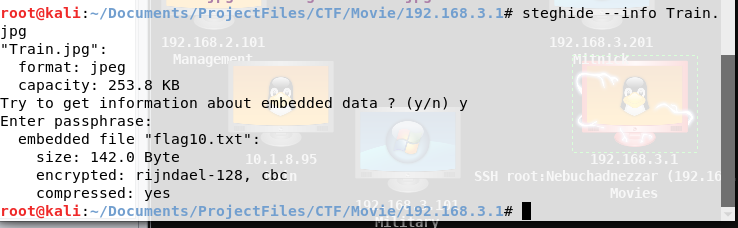


* We then opened the flag9.pst file in Outlook, which contained the following email, with the attachment “flag9.txt”

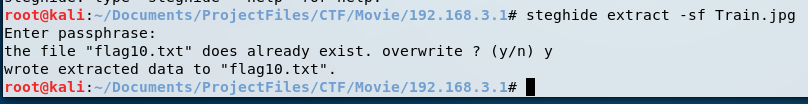


**Flag10:**

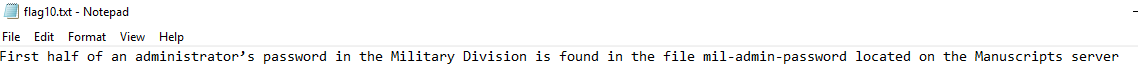
* Using the previously decoded steganography password – 37568727, we used “steghide –info filename” to detect stego on each downloaded image from the web server. The Train.jpg file had an embedded file “flag10.txt”



* We used “steghide –extract Train.jpg” to extract the flag10.txt file:



* Flag 10 is shown below:



How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
| root |  | Nebuchadnezzar |
| trinity |  | Z1ON0101-matrix~dragon7 |
| matrix |  | TakeTheRedPill# |
| neo |  | I5Th0mas4nd3rson |
| switch |  | Letmein!please |

**Military Division 192.168.3.101**

How did you find the target?

How did you gain access to the target?

* Once we opened a Meterpreter shell on Movie, we used “setup pivot” to pivot to

How did you learn usernames?

How did you learn passwords?

How did you find and download flags?

**Flag11:**

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
| JuliusCaesar |  |  |
| Bullwinkle |  | E$Rft6avgga!4zB^ |
| OptimusPrime |  |  |
| Administrator |  |  |

**Medical Division – 172.22.22.1**

How did you find the target?

How did you gain access to the target?

* Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.
* If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
* What tool(s) or commands did you use to exploit the system?

How did you learn usernames?

How did you learn passwords?

How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
| MartyMcfly |  | fluxcapacitor |
| Cypher |  | envelopesurgeon |
|  |  |  |
|  |  |  |

Launching exploit manually through Medical to Meteorology

**Meteorology Division**

How did you find the target?

How did you gain access to the target?

* Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.
* If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
* What tool(s) or commands did you use to exploit the system?

How did you learn usernames?

How did you learn passwords?

How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Mitnick Division – 192.168.3.201**

How did you find the target?

How did you gain access to the target?

* We used a SET payload/listener and emailed it to [DavidKennedy1@mail.m4i.local](mailto:DavidKennedy1@mail.m4i.local)
* This payload spawned a meterpreter shell into the device

How did you learn usernames?

* We executed the “run hashdump” command to dump the hashes for each user on the machine, and pulled off the users from that list.

How did you learn passwords?

* We ran the Mitnick hashes through Ophcrack. This showed us the last part of each LM hash (REEHUGS and 4CK3R)
* We searched ChrisHadnagy on Twitter, and saw his username was “ReLik”
* We made a custom character list for a brute force attack in Cain, and found the passwords

How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
| DavidKennedy |  | Relik freehugs |
| ChrisHadnagy |  | HUMAN H4CK3R |

**Marconi Division**

How did you find the target?

How did you gain access to the target?

* Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.
* If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
* What tool(s) or commands did you use to exploit the system?

How did you learn usernames?

How did you learn passwords?

How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Make Division**

How did you find the target?

How did you gain access to the target?

* Open ports used during your pen test. Provide a listing of the open ports/services you actually used. You are not required to report ports you did not use. Do not forget the command used to execute the scan.
* If you used an exploit against a computer, list the vulnerabilities you used and what tool you used to find the vulnerabilities.
* What tool(s) or commands did you use to exploit the system?

How did you learn usernames?

How did you learn passwords?

How did you find and download flags?

How did you find and download any other files you may have harvested from the target?

|  |  |  |
| --- | --- | --- |
| **Username** | **Account Type** | **Password** |
| TEdison |  | Moviecreator |
| user |  | user |
|  |  |  |
|  |  |  |

**Table of all usernames and passwords:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Division** | **Username** | **Account Type** | **Password** |
|  |  |  |  |  |
|  |  |  |  |  |

**Appendix A: Supplemental Questions**

1. List the restaurants Dr. Evil visits frequently
2. What is the password learned from the Heartbeat Server

**Appendix B: Source Code**



**General Observations:**

* You are required to keep a log of time spent on this assignment and include the log in this appendix.
* How long (in wall clock hours; not man hours) did it take to complete the project excluding the report?
* How long (in wall clock hours; not man hours) did it take to prepare the report?
* Was it an appropriate length final assignment considering the time allotted?
* What corrections and or improvements do you suggest for this project?
  + Please be specific, and if you add new material, give the exact wording/instructions you would give future students in the new project handout. Feel free to cross out and edit text to make minor corrections/suggestions.